⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－131169

⑤Int.Cl.⁴	識別記号	庁内整理番号	④公開　昭和63年(1988)6月3日
G 09 C 1/00		7368－5B	
G 06 F 12/00	302	R－6711－5B	
12/14	320	B－7737－5B	審査請求　未請求　発明の数 1　（全5頁）

⑤発明の名称　暗号データ復号化方式

⑳特　願　昭61－276524
㉒出　願　昭61(1986)11月21日

㉗発明者　内藤　一郎　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
㉗発明者　前沢　裕行　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
㉔代理人　弁理士　小川　勝男　外1名

明　細　書

1．発明の名称

暗号データ復号化方式

2．特許請求の範囲

1．ファイルメモリに蓄積された暗号データを、復号鍵情報を用いて平文データに復号化する手段を有する計算機システムにおいて、記憶機能を有するカードに記録された復号鍵情報を入力する手段と、この復号鍵情報を用いて、ファイルメモリ内の暗号化されたデータを参照して平文データに復号化する手段、を有することを特徴とする暗号データ復号化方式。

2．記憶機能を有するメモリカードに記憶された暗号鍵情報を入力し、この情報を用いて平文データを暗号データに暗号化して、ファイルメモリに書換する手段を加えたことを特徴とする請求範囲第1項記載の暗号データ復号化方式。

3．記憶機能を有するメモリカードに記憶された復号化アルゴリズムを入力する手段と、この復号化アルゴリズムを用いて、ファイルメモリ内の暗号化されたデータを参照して平文データに復号化する手段を加えたことを特徴とする請求範囲第1項記載の暗号データ復号化方式。

4．暗号鍵情報と復号化プログラムを記録した記憶機能と、プログラム実行機能とを備えたメモリカードを計算機システムに装填し、計算機システム内のファイルメモリ内の暗号データを、メモリカード内の復号化プログラムをメモリカード内で実行して平文データに復号化する手段を備えたことを特徴とする、請求範囲第1項記載の暗号データ復号化方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本方式は電子計算機方式に係り、特に複数の利用者が1つの計算機システムを利用する場合、計算機システム内のファイル内容の機密保護に好適な暗号データ復号化方式に関する。

〔従来の技術〕

複数の利用者が使用する電子計算機システムにおいては、特定の利用者が専用するファイル内の

データを，悪意を持つ他の利用者が使用することを防止する必要がある。

この問題を解決するため，従来次のような方式があつた。

(1) 利用者毎に，識別名称やパスワードを定めて計算機システム内に保持し，計算機使用時に利用者が指定する識別名称，パスワードと照合することにより，利用者の計算機使用権限をチエックする手段と，計算機システム内の各ファイル毎に，ファイルを利用できる利用者の識別名称等を保持する情報を計算機システム内に保持し，この情報により利用者の，使用を要求するファイルの使用資格をチエックする手段を設ける方式。

(2) ＩＣカード，レーザーカード，磁気カード等の，情報を記憶することが可能なカードに，当該カード所有者が使用できる少なくとも１以上のファイルの識別名称等や，利用者の識別名称，パスワード等を記憶し，利用時に，このカード内の情報を入力して，利用者の計算機利用資格や，使用を要求したファイルへのアクセス資格をチエックする手段を設ける方式。

(3) ファイルにデータを書き込む時に，データを公知の方式により暗号データに変換して，ファイルに蓄積し，参照する際は，逆変換して，平文データに直す手段を設ける方式。

〔発明が解決しようとする問題点〕

しかし上記従来技術には，次のような問題が存在した。

上記(1)の従来技術には，利用者の識別名称やパスワード等が，他者に知られないことを前提としている。この情報が計算機利用時の利用者入力や，あるいは計算機内に蓄積された利用者識別名称情報等を参照することにより，他者に盗まれる恐れがある。

上記(2)の従来技術は，利用者の識別名称やパスワード，及びファイルへのアクセス資格等の情報をＩＣカード等の情報が記憶可能なカードに記憶し，この情報を計算機使用時に入力してファイルアクセス権限を得る方式であり，その情報を視覚により知ることが出来ない。またこの情報は計算機内には常時は蓄積されていないので，他の利用者がこれを知つて，他者のファイルへのアクセス権限を得ることは難しくなる。

しかし一般の計算機システムでは，計算機管理者のため，あらゆるファイルにアクセスを可能にするマスタとなる識別名称やパスワードを設けている。従つて計算機管理者や，あるいは計算機管理者からマスタとなる識別名称やパスワードを盗んだ者が，機密情報を保持するファイル内のデータを参照して盗む恐れがある。

上記(3)の従来技術は，ファイルデータ自体を暗号化することにより，ファイルのアクセス権限を盗んだ他者が，ファイル内のデータを参照してもそのデータの意味を理解できなくすることを狙つたものである。しかしこの方式においても暗号データを平文データに変換するための復号化アルゴリズムと，そのアルゴリズムで使用する，復号鍵情報を他者に知られた時は，このファイル内データを解読されてしまう。復号化アルゴリズムは計算機内にプログラムとして蓄積され，復号鍵情報は計算機内にデータとして蓄積されているか，あるいは利用時に入力されるので，両者とも，他者に知られる恐れが残されている。

本発明の目的は，計算機システム内のファイル内に蓄積された，暗号化されたデータを他者に盗まれる恐れなく平文化して使用しうる手段を提供することにある。

〔問題点を解決するための手段〕

上記目的は，ＩＣカード，レーザーカード，磁気カード等の記憶可能なカードに記憶された復号鍵情報を，暗号データを保持するファイル使用時に入力する手段と，暗号データ保持ファイルから入力した暗号データを，該復号鍵情報と復号化アルゴリズムを用いて平文データに変更する手段とにより達成される。

〔作用〕

暗号データを復号化するための復号鍵情報は，当該ファイルの使用権をもつ利用者のカード内にのみ保持される。従つて，他者が計算機システム

内の情報を調べたり，あるいは利用者の復号鍵情報を盗み見たりすることにより，復号鍵情報を知ることができない。このため，機密データを蓄積したファイルへのアクセス権を得，更に復号化アルゴリズムをも知つた他者が，当該ファイル内の暗号データを参照しても，最終的にこれを平文データに変換することが阻止されるので，他者による悪用を効果的に防止することが出来る。

〔実施例〕

以下，本発明の一実施例を図面を用いて詳細に説明する。本実施例はデータの暗号化・復号化に同一の鍵情報を利用し，暗号化・復号化のアルゴリズムは計算機内に保持されたプログラムにより実現する例である。

第１図に本実施例を実現するシステムの機能構成図を示す。１は暗号化・復号化の両方に使用する鍵情報を記録したメモリカードである。２は１のメモリカード内の情報を入力して蓄積部３に蓄積する入力部である。５はキーボード４より平文データを入力するデータ入力部である。６は暗号化部であり，入力部５により入力された平文データを蓄積部３に蓄積された鍵情報と暗号化部６自体に内蔵された公知の暗号化ロジックを用いて暗号データに変換する部分である。７は暗号化されたデータをファイル８内に書込む部分である。

９はファイル８内の暗号データを読み込む部分，１０はデータ復号化部でありデータ読込部９により得られた暗号データを蓄積部３の鍵情報と復号化部１０自体に内蔵された公知の復号化ロジックを用いて平文データに変換する部分である。１１は復号化部１０で得られた平文データをプリンタ１２に出力する部分である。

第１図の機能構成図において，ファイルメモリに暗号データを書き込む処理のフローチャートを第２図に示す。

まず処理１３ではメモリカードの内容を計算機システムに入力する。処理１４～１７ではキーボードよりデータを入力しては暗号化してファイルに書込む処理を繰返す。即ち，処理１４ではキーボードより平文データ又は入力終了通知データを入力する。処理１５では入力されたデータが入力終了通知データかを判断する。もし入力終了通知データでなければ，処理１６において，平文データを暗号データに変換する。処理１６は第１図の暗号化部６に対応する。この処理は，メモリカードから入力された鍵情報と，暗号化部６に内蔵された暗号化ロジックとを用いて，平文データを暗号データに変換する処理である。第２図処理１７では上述の如くして暗号化されたデータをファイルに書込む。処理１４～１７を入力終了通知データが入力されるまで繰返し，入力終了通知データが入力されれば，１５の判定処理により終了する。

ファイル・メモリより暗号手段を読み出す処理のフローチャートを第３図に示す。

まず処理２０ではメモリカードの内容を計算機システムに入力する。処理２１～２４でファイルより暗号データを読み出し，復号化してはプリンタに出力する処理を繰り返す。処理２１ではファイルより暗号化されたデータまたはファイル終了データ（ＥＯＦ）を読みこむ。処理２２では読みこまれたデータが，暗号化されたデータかファイル終了データかを判断する。もし暗号化されたデータであれば，２３においてこのデータを平文データに変換する。２３の処理は第１図の復号化部１０に対応する。この処理は，メモリカードから入力された鍵情報と復号化部１０に内蔵する復号化ロジックを用いて暗号データを平文データに変換する処理である。第３図処理２４により平文化されたデータをプリンタに出力する。２１～２４の処理をファイル終了データがファイルから読み込まれるまで繰返す。ファイル終了データが読み込まれれば処理２２の判定処理により終了する。

上記の実施例は，暗号化，復号化に用いる鍵を同一にしてメモリカードにもたせることにより，暗号化・復号化の操作の簡便化を計つている。

次に暗号化・復号化のロジックをもメモリカードにもたせた実施例を示す。機能構成図を第４図に示す。図において符号の３～５，７～９，１１～１２の部分は第１図と同じである。

メモリカード３０は鍵情報の他に，暗号化プロ

グラム，復号化プログラムの情報を保持する。入力部３１はカード３０より鍵情報，暗号化プログラム，復号化プログラムを入力しそれぞれを鍵情報蓄積部３，暗号化部３２，復号化部３３に蓄積する。暗号化部３２の処理は第１図６と同様であるが，メモリカード３０で入力された暗号化プログラム内のロジックに従つて暗号データを作成する点が異なる。復号化部３３の処理も，第１図復号化部１０と同様であるが，メモリカードで入力された復号化プログラム内のロジックに従つて平文データを作成する点が異なる。

ファイルメモリ８に暗号データを書きこむ処理手順，ファイルメモリより暗号データを読み出す処理手順は，第１図の実施例の場合と同様，それぞれ第２図，第３図のフローチャートであらわされる。

本実施例では，暗号化ロジック，復号化ロジックをもメモリカードに記録し，必要時のみ計算機システムに蓄積することにより，両ロジックを秘密にすることができる。従つて暗号データを解読される恐れは一層減少する。

更にメモリカード内にプロセッサを保持し，データ暗号化や復号化を，計算機システムに装填したメモリカード内で実行する方式も考えられる。

第５図に本実施例の機能構成図を示す。図の符号４～５，７～９，１１～１２は第１図の実施例と同様である。１１はプロセッサを内蔵したメモリカードであり，計算機システム４０に装填されている。４２はメモリカードに内蔵した暗号化プログラムであり，入力部５から得た平文データを，蓄積部４１の鍵情報を用いて暗号データに変換してデータ書込部７にわたす。４３はメモリカードに内蔵した復号化プログラムであり，データ読込部９より得た暗号データを鍵情報蓄積部４１を用いて平文データに変換して出力部１１に渡す，

利用者はデータ暗号化，復号化の際にのみメモリカードを計算機システムに装填すればよい。

本実施例によれば，鍵情報や暗号化ロジック・復号化ロジックが計算機システム内に一時的にも蓄積されることがないため機密データの保護が一層完全になる。

〔発明の効果〕

以上説明したように，本実施例によれば，暗号化されてファイル内に蓄積されたデータを復号化するための鍵情報を他者が知ることができないため，計算機内のファイルメモリに保持された機密データの保護性能の向上を計ることが出来る。

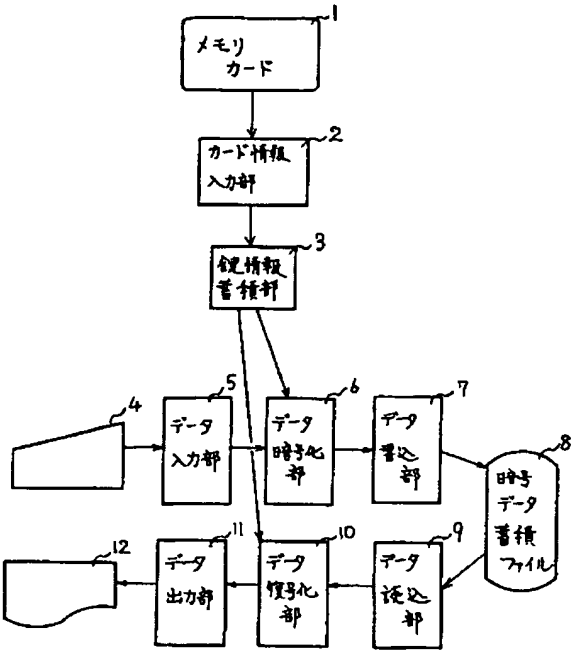
４．図面の簡単な説明

第１図は本発明の一実施例の機能構成図，第２図はデータ入力処理のフローチャート，第３図はデータ出力処理のフローチャート，第４図は第２の実施例の機能構成図，第５図は第３の実施例の機能構成図，である。

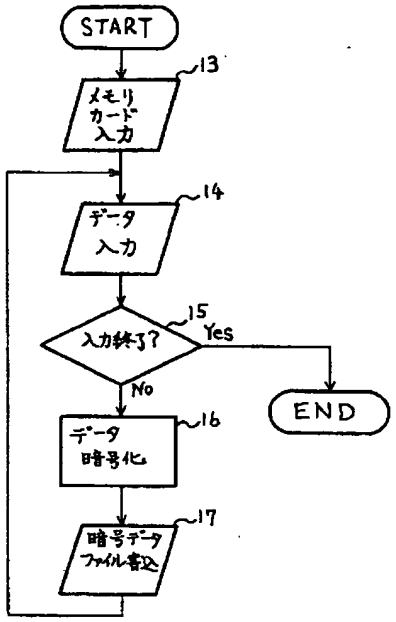
１…メモリカード，２…カード情報入力部，６…データ暗号化部，７…データ書込部，８…暗号データ蓄積ファイル，９…データ読込部，１０…データ復号化部。

代理人　弁理士　小川勝男

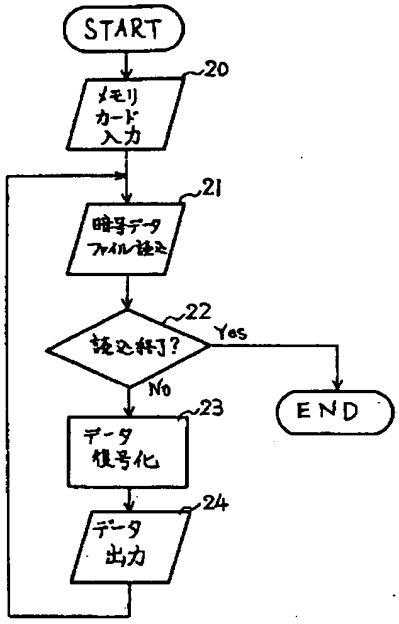
第　１　図



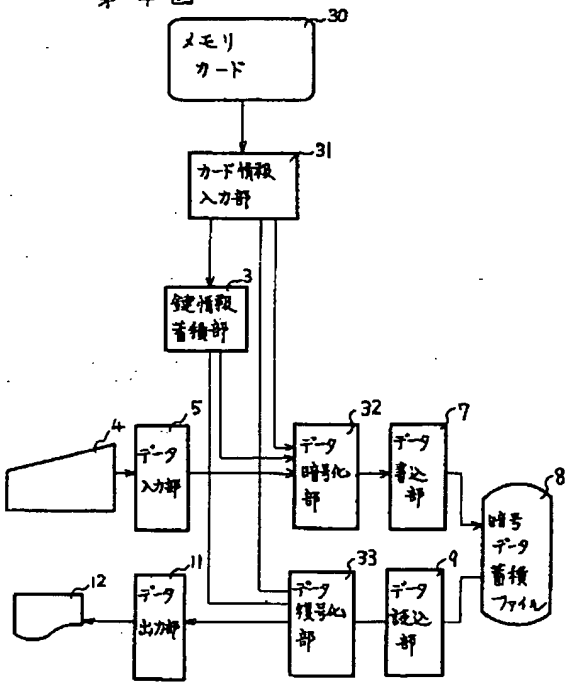
第 2 図



第 3 図

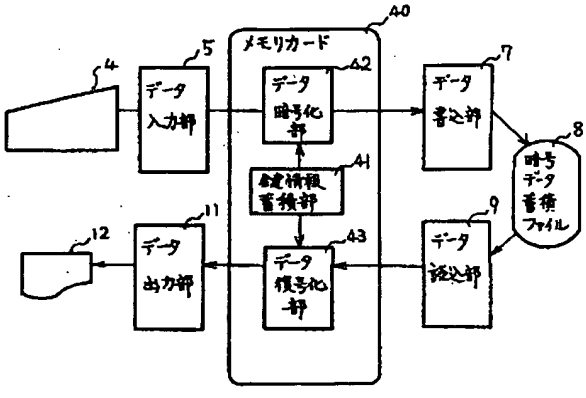


第 4 図



31 カード情報入力部
32 データ暗号化部
33 データ復号化部

第 5 図



40 メモリカード
41 鍵情報蓄積部
42 データ暗号化部
43 データ復号化部